NEEL CHATTERJEE (SBN 173985)
NChatterjee@goodwinlaw.com
GOODWIN PROCTER LLP
601 Marshall Street
Redwood City, CA 94063
Tel. +1 650 752 3100
Fax: +1 650 853 1038

SHARON R. SMITH, (SBN 221428)
SharonSmith@goodwinlaw.com
MEGAN D. BETTLES (SBN 328161)
MBettles@goodwinlaw.com
GOODWIN PROCTER LLP
Three Embarcadero Center, Suite 2800
San Francisco, CA 94111
Tel.: +1 415 733 6000
Fax: +1 415 677 9041

Attorneys for Defendants
PASSES, INC. and LUCY GUO

IN THE UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

FAMOUS BIRTHDAYS, LLC, a California limited liability company,

Plaintiff,

v.

PASSES, INC., a Delaware corporation; and LUCY GUO, an individual,

Defendants.

Case No. 2:24-cv-08364-AS

DECLARATION OF MARKUS JAKOBSSON, PH.D. IN SUPPORT OF OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

Date: December 3, 2024
Time: 10:00 a.m.
Ctrm.: 8-D
Judge: Hon. Consuelo B. Marshall

Action Filed: September 27, 2024

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

DECLARATION OF MARKUS JAKOBSSON, PH.D.

I, Markus Jakobsson, Ph.D., hereby state and declare:

1. I am a computer and network security expert. I have been retained by Lucy Guo ("Ms. Guo") and Passes, Inc. ("Passes") to analyze factual information relating to certain allegations made by Famous Birthdays, LLC ("Famous Birthdays") in its Motion for a Preliminary Injunction and supporting papers. I submit this Declaration in connection with Passes' Opposition to Plaintiff's Motion for a Preliminary Injunction (the "Opposition").

2. I make this Declaration based upon my own personal knowledge, information, and belief, and I would and could competently testify to the matters set forth in this Declaration if called upon to do so.

3. As I explain in more detail below, based on the information available to me to date and my expertise, I've reached five conclusions :

i. Passes did not "surreptitiously extract [the historical rank graph API call] from the Famous Birthdays source code." Ostrowski Decl., ¶ 29; *infra* ¶ 22.

ii. The rank graph API endpoint was not "internal" only to Famous Birthdays. Ostrowski Decl., ¶ 26.

iii. Passes did not insert anything "amidst Famous Birthdays Pro's source code," or otherwise alter Famous Birthdays source code. Ostrowski Decl., ¶ 27.

iv. The access log in no way "reflect[s] that Passes used an automated script that pretended to be an authorized human Passes' user of Famous Birthdays Pro with permission to use Passes' Famous Birthdays [access]." Ostrowski Decl., ¶ 35.

v. The list of Famous Birthdays URLs can be compiled by anyone, with or without access to Famous Birthdays Pro services, because Famous Birthdays' sitemap is public. Ostrowski Decl., ¶ 33.

Overall, any identification and use of a rank graph API call by Passes was

technologically authorized, reasonable, did not harm any Famous Birthdays' computer systems or code, and should have been anticipated by Famous Birthdays.

QUALIFICATIONS AND EXPERIENCE

4. I have twenty-five years of experience as a security researcher and scientist studying phishing, crimeware and mobile security at organizations such as PayPal, Palo Alto Research Center (PARC), Qualcomm, RSA Security and ByteDance. I have co-founded four digital security startups spanning email fraud prevention, user authentication, mobile malware detection and secure user messaging. I have a Ph.D. in computer science from the University of California at San Diego, as well as master's degrees from both the University of California at San Diego and Lund University in Sweden.

5. I hold over 200 patents and more than 200 pending patents, all related to computer security, network security, or both. For the entirety of my career, I have focused on various issues related to computer and network security. I have been retained in numerous cases as an expert in computer science, forensics, and security.

6. I am currently the Chief Scientist at Artema Labs, a crypto startup concerned with the security and confidentiality of digital representations of ownership. My research relates to how to make online transfers of ownership secure against abuses of various types, among other things.

7. I am also the CEO at ZapFraud, a cybersecurity company that develops techniques to detect deceptive emails, such as Business Email Compromise emails. At ZapFraud, my research studies and addresses abuse, including social engineering, malware and privacy intrusions. My work primarily involves identifying risks, developing protocols and user experiences, and evaluating the security of proposed approaches.

8. I received a Master of Science degree in Computer Engineering from the Lund Institute of Technology in Sweden in 1993, a Master of Science degree in Computer Science from the University of California at San Diego in 1994, and a

Ph.D. in Computer Science from the University of California at San Diego in 1997, specializing in Cryptography. During and after my Ph.D. studies, I was also a Researcher at the San Diego Supercomputer Center, where I did research on authentication and privacy.

9. From 1997 to 2001, I was a Member of Technical Staff at Bell Labs, where I did research on authentication, privacy, multi-party computation, contract exchange, digital commerce including crypto payments, and fraud detection and prevention. From 2001 to 2004, I was a Principal Research Scientist at RSA Labs, where I worked on predicting future fraud scenarios in commerce and authentication and developed solutions to those problems. During that time I predicted the rise of what later became known as phishing. I was also an Adjunct Associate Professor in the Computer Science department at New York University from 2002 to 2004, where I taught cryptographic protocols.

10. From 2004 to 2016, I held a faculty position at the Indiana University at Bloomington, first as an Associate Professor of Computer Science, Associate Professor of Informatics, Associate Professor of Cognitive Science, and Associate Director of the Center for Applied Cybersecurity Research (CACR) from 2004 to 2008; and then as an Adjunct Associate Professor from 2008 to 2016. I was the most senior security researcher at Indiana University, where I built a research group focused on online fraud and countermeasures, resulting in over 50 publications and two books.

11. While a professor at Indiana University, I was also employed by Xerox PARC, PayPal, and Qualcomm to provide thought leadership to their security groups. I was a Principal Scientist at Xerox PARC from 2008 to 2010, a Director and Principal Scientist of Consumer Security at PayPal from 2010 to 2013, a Senior Director at Qualcomm from 2013 to 2015, Chief Scientist at Agari from 2016 to 2018, Chief of Security and Data Analytics at Amber Solutions from 2018 to 2020, and Chief Scientist at ByteDance from 2020 to 2021.

12. Agari is a cybersecurity company that develops and commercializes technology to protect enterprises, their partners and customers from advanced email phishing attacks. At Agari, my research studied and addressed trends in online fraud, especially as related to email, including problems such as Business Email Compromise, Ransomware, and other abuses based on social engineering and identity deception. My work primarily involved identifying trends in fraud and computing before they affected the market, and developing and testing countermeasures, including technological countermeasures, user interaction and education.

13. Amber Solutions is a cybersecurity company that develops home and office automation technologies. At Amber Solutions, my research addressed confidentiality, user interfaces and authentication techniques in the context of ubiquitous and wearable computing, and involved the tracking of users, for purposes of personalization and emergency response.

14. ByteDance is a media company concerned with secure processing of data, and is the owner of TikTok. At ByteDance, my research addressed fraud prevention, confidentiality, user interfaces and authentication techniques in the context of the many products offered by ByteDance.

15. I have founded or co-founded several successful computer security companies. In 2005 I co-founded RavenWhite Security, a provider of authentication solutions, and I am currently its Chief Technical Officer. In 2007 I co-founded Extricatus, one of the first companies to address consumer security education. In 2009 I founded FatSkunk, a provider of mobile malware detection software; I served as Chief Technical Officer of FatSkunk from 2009 to 2013, when FatSkunk was acquired by Qualcomm and I became a Qualcomm employee. In 2013 I founded ZapFraud, a provider of anti-scam technology addressing Business Email Compromise, and I am currently its CEO. In 2014 I co-founded RightQuestion, a company concerned securing telecommunications. In 2023, I co-founded CSExpert,

a security consulting company, and Security Technology, a company addressing multiple consumer-facing technology needs, including improvements of targeted advertising methods.

16. I have additionally served as a member of the fraud advisory board at LifeLock (an identity theft protection company); a member of the technical advisory board at CellFony (a mobile security company); a member of the technical advisory board at PopGiro (a user reputation company); a member of the technical advisory board at MobiSocial dba Omlet (a social networking company); and a member of the technical advisory board at Cequence Security (an anti-fraud company, previously named Stealth Security). I have provided anti-fraud consulting to KommuneData (a Danish government entity), J.P. Morgan Chase, PayPal, Boku, and Western Union.

17. I have authored six books and over 100 peer-reviewed publications.

18. My work has included research in the area of applied security, confidentiality, cryptographic protocols, authentication, malware, social engineering, usability and fraud prevention.

19. I have been engaged as a technical expert in over 75 computer-related cases, including numerous cases involving Internet security, mobile security, forensics, code analysis, encryption and/or authentication.

MATERIALS CONSIDERED

20. In forming my opinions, I read the Declaration of Kevin Ostrowski in Support of Motion for an Order Issuing a Preliminary Injunction (Dkt. 10-1, the "Ostrowski Decl.") and Declaration of Evan Britton in Support of Plaintiff's Application for Leave to File Under Seal Certain Exhibits to Kevin Ostrowski's Declaration in Support of Motion for an Order Issuing a Preliminary Injunction (Dkt. 10, the "Britton Sealing Decl."). I disagree with multiple statements made therein, particularly the suggestion that Ms. Guo and Passes engaged in any sort of hacking activity.

21. To prepare the Opposition, I understand that Passes and Ms. Guo requested further information from Famous Birthdays and it was not provided. Because Famous Birthdays did not provide these documents, I cannot opine on some of the exact documents that Famous Birthdays ostensibly relied on in making the assertions in the Britton and Ostrowski Declarations.

OPINIONS

A. FIRST, PASSES DID NOT "EXACT" THE RANK GRAPH API ENDPOINT FROM FAMOUS BIRTHDAYS' SOURCE CODE.

Background: API Endpoints

22. An API, or an Application Programming Interface, is an interface that enables a computer to access data stored on a server, much like how a webpage is part of an interface that a person can access data stored on the server. APIs are commonly used to enable a service to access other services. An API endpoint is the URL that specifies the address of the API, similar to how a webpage is accessed through its URL.

The Rank Graph API Endpoint is Publicly Visible in Network Mode

23. Famous Birthdays' assertion that Passes "surreptitiously extracted [historical rank graph API call] from the Famous Birthdays source code" is wrong. *See* Ostrowski Decl., ¶ 29. Nothing needed to be "extracted from the Famous Birthdays source code." The rank graph API endpoint can be readily observed by anyone using the Network tab in a browser developer tool, like Chrome Developer Tools. This functionality is available to anyone who uses the well-known tools for Chrome, a set of tools provided by Google.

24. Famous Birthdays' Mr. Ostrowski also discusses "internal API endpoints were not shared with Passes," and asserts that that "obtain[ing] one of th[o]se API endpoints" "can only be done" through "accessing Famous Birthdays' backend code or reverse engineering its system." *See* Ostrowski Decl., ¶¶ 25, 26. Based on the information that I have reviewed, I have no reason to believe that Passes

"access[ed] Famous Birthdays' backend code or reverse engineer[ed] its system." Instead, it is my understanding that Passes identified the rank graph API endpoint by using the Network tab in a browser developer tool, like Chrome Developer Tools.

25. A person can find this API endpoint with a browser development tool without being "sophisticated in computer science" or needing to "pull[] up Famous Birthdays source code." *See* Ostrowski Decl., ¶ 26. Anybody with a computer equipped with a browser can do this. First, a user who logs into Famous Birthdays Pro can open its browser's developer tools and navigate to the "Network" tab. Once in the Network tab, the user can view all network activity as it interacts with the page, including observing API calls such as data requests and responses between the browser and server. By filtering for "XHR" or "Fetch" requests, the user can access details like endpoint URLs, request methods, headers, payloads, and server responses, providing insight into the data exchange without needing access to the underlying code that triggers these interactions.

26. Simply viewing network activity, which is displayed in HTML code (which is generally readable in plain language), is unrelated to accessing or interacting with source code. Viewing network activity involves observing data exchanges between the browser and server, while accessing source code requires direct interaction with the underlying code that defines how the system operates.

27. Part of the reason I conclude Passes did not access Famous Birthdays' backend code or reverse engineer its computer system is because the rank graph API endpoint is not an "internal" endpoint at all. I describe this further, below. *Infra*. Sec. B.

Passes' Identification of the Rank Graph API Endpoint Was Not Surreptitious

28. Any access to the Famous Birthdays Pro system or actions taken by Passes while logged in was not "surreptitious." *See* Ostrowski Decl., ¶ 29. Because Passes (a Famous Birthdays Pro user) must provide credentials to log into Famous Birthdays Pro, Passes' access to the Famous Birthdays Pro services is traceable.

29. It is unclear what makes Passes' accesses surreptitious in the minds of Famous Birthdays; after all, the accused accesses appear to have been made using the web interface that Famous Birthdays developed, and there is no indication that Passes attempt to hide its access.

B. SECOND, THE RANK GRAPH API ENDPOINT IS NOT INTERNAL.

Background: Internal vs. External API Endpoints

30. The difference between an "external" (or publicly accessible) API endpoint and an "internal" API endpoint lies in who can access the resources behind the endpoint. A publicly accessible endpoint can be accessed by a member of the public. In contrast, an "internal" API access point can only be accessed by somebody authorized to gain full access to the corresponding server, such as a company's trusted systems administrator managing the server. This makes it possible to have API endpoints that can only be used by select employees. These are typically used to enable privileged operations that the public is not granted rights to. The use of the term "internal" typically refers to infrastructure which is not directly accessible to non-privileged users unless the user engages in some sort of hacking activity to circumvent access limitations and is inapplicable here

Internal Endpoint

31. Famous Birthdays' characterization of the rank graph API as an "internal API endpoint" is incorrect. *See* Ostrowski Decl., ¶ 27.

32. The rank graph API appears to be accessible to anybody logged into Famous Birthdays Pro. For the rank graph API, I am unaware of any information suggesting that internal Famous Birthdays employee credentials were required, and Famous Birthdays does not provide any evidence to support that assertion.

33. Additionally, the rank graph API endpoint has the same structure as the other API endpoints that Famous Birthdays admits it provided Passes and other customers. *Compare* Ostrowski Decl., Ex. B ("[redacted]

[redacted]") *with* Ostrowski Decl., Ex. B ("[redacted]").

34. Unless there are security restrictions placed on an API endpoint, any Famous Birthdays Pro user can then access the API endpoint listed in the HTML code simply by calling it manually or through a simple script. Calling an API endpoint also does not require knowledge of the Famous Birthdays source code.

C. THIRD, PASSES DID NOT PLACE THE RANK GRAPH API CALL "AMIDST" FAMOUS BIRTHDAYS PRO'S SOURCE CODE.

Background: API Calls and Source Code

35. API calls are also not somehow "inserted in" source code. An API call is a request that is sent over a network, to the API, and contains requests for information. In the same way that an email that sent from one user to another does not become part of the recipient, it is not meaningful to speak of inserting API calls in code of a server. Famous Birthdays' insinuation that someone could alter Famous Birthdays' source code by inserting "this API call amidst Famous Birthdays Pro's source code," is wrong because API calls are *made*. *See* Ostrowski Decl., ¶ 27. Moreover, I have not heard any evidence that Famous Birthdays' servers have been compromised, whether in the context of the accused access or not.

The API Call Shown in Exhibit C to Ostrowski Declaration Was Not Made by Passes

36. Moreover, there is no information provided that indicates that the screenshot attached as Exhibit C to the Ostrowski Declaration reflects an API call made by Passes. The rank graph API call shown in this screenshot could have been made by anyone with access to Famous Birthdays Pro. The "rank graph" reference on the fourth row from bottom does not show who or how the page was accessed, but the screenshot does show when. Based on the date-stamp of the graph on the page, it appears that this access was made in October 2024, which I understand was months

after Famous Birthdays terminated Passes access. This suggests that the screenshot may have been taken by Famous Birthdays, reflecting their own access to their own system and their own use of the rank graph API call.

Exhibit C Does Not Show Any of Famous Birthdays' Source Code

37. I strongly disagree with Mr. Ostrowski's assertion this screenshot "show[s] this internal API call amidst Famous Birthdays Pro's source code." *See* Ostrowski Decl., ¶ 27, Ex. C. Mr. Ostrowski's statement demonstrates a fundamental misunderstanding how API calls work. This screenshot shows somebody accessing a particular page on Famous Birthdays Pro, while using the Network tab in Chrome Developer Tools. This is functionality available to anyone who uses the well-known tools for Chrome, a set of tools provided by Google. On the right side, a set of web server requests are shown, along with their status (e.g., 200, which is also referred to as HTML 200 OK, and which corresponds to a request that was accepted).

38. The HTML code shown in the Network tab is not in any way the same as "Famous Birthdays source code." *See* Ostrowski Decl., ¶ 27, Ex. C; *see also supra* at ¶¶ 25-27. This screenshot does not show any source code at all. As such, I disagree that "[t]his screenshot also shows back-end source code that populates Famous Birthdays Pro." *See* Britton Sealing Decl., ¶ 7.

There Is No Evidence that Passes' Use of the Rank Graph API Altered Famous Birthdays' Source Code

39. Famous Birthdays' evidence does not suggest or indicate in any way that Passes introduced any API or in any way altered Famous Birthdays source code. The excepted use of the Famous Birthdays rank graph API call by Passes would not alter Famous Birthdays source code, and I have not seen any evidence to the contrary. The apparent functionality of the Famous Birthdays rank graph API is to provide access to information related to a specific public figure with a profile in Famous Birthdays' database, such as whether the public figure is trending upwards or downwards in popularity, the public figure's social media handles.

D. FOURTH, FAMOUS BIRTHDAYS' ACCESS LOGS DO NOT SHOW PASSES "PRETEND[ING] TO BE AN AUTHORIZED HUMAN" OR SHOW "PASSES MADE VERBATIM COPIES OF THE WORKS."

Background: Access Log

40. An access log comprises a list of records, each record corresponding to one request. There can be logs corresponding to webpage based requests (which are made as a webpage is rendered on a user browser) or based on requests to APIs. A record of an access log typically indicates the IP address from which the request was made, the time of the request, what the request was, and whether the request was successful. Access logs can also contain information about what user or process is making the request. Most web servers are configured to automatically generate access logs.

The Access Log Only Shows API Calls Made

41. I disagree with Famous Birthdays' assertion that "[t]he access logs reflect that Passes used an automated script that pretended to be an authorized human Passes user of Famous Birthdays Pro with permission to use Passes' Famous Birthdays API token." *See* Ostrowski Decl., ¶ 35. Famous Birthdays provided no explanation for how an automated script can "pretend" to be a human and provided no evidentiary support for its assertion that the script "pretended" to be a human.

42. To the extent that Famous Birthdays indicate that they use some form of technology that distinguishes automated accesses from human-initiated accesses (such as a CAPTCHA does), I am not aware of Famous Birthdays using any such technology on its website. It would, however, be bizarre to have a CAPTCHA to verify that an API access corresponds to a human, since the very intention of an API is to act as an interface to other computers. If the APIs on Famous Birthdays Pro's website had such controls, it would render the APIs practically useless for any of their customers. To the extent, however, that they do have such a control

implemented, I have not been made aware of any evidence that it was violated by Passes.

43. I also disagree with Famous Birthdays' assertion that "Famous Birthdays has server logs demonstrating Passes made verbatim copies of the Works." Motion at 25:10-11. The only log provided by Famous Birthdays is the access log attached as Exhibit D to the Ostrowski Declaration. That log does not demonstrate that Passes made any copies, instead it shows a list of records of requests to the rank graph API endpoint. In fact, since the access logs are made by the server (e.g., Famous Birthdays' server) and a potential copy of received information is supposedly made by the party accessing the server (i.e., on a remote system to which the server does not have any insight into how received data is processed) it is a very strange assertion that the logs indicate that copying was made.

E. FIFTH, THE SITEMAP FOR FAMOUS BIRTHDAYS' WEBSITE IS PUBLIC.

Background: Sitemap

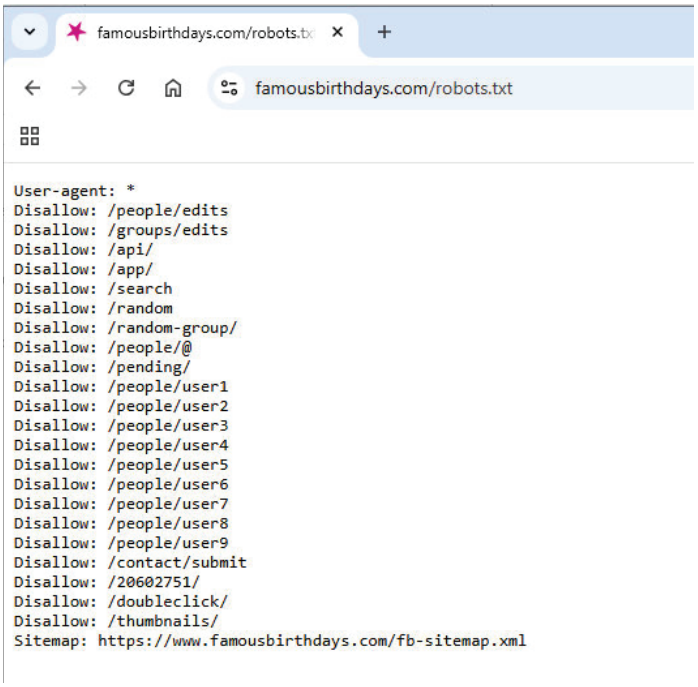
44. A sitemap is a file that provides a structured list of all the important pages on a website, helping search engines understand and efficiently crawl its content. It can also include metadata about each page, such as when it was last updated and its relevance. Many companies keep their sitemaps hidden or restrict access if they do not want certain information to be publicly available. This can be achieved by placing the sitemaps in non-public directories or employing other methods to limit visibility, ensuring that sensitive data about their site's structure remains private and less discoverable.

Any Member of the Public Can Obtain a List of Famous Birthdays' URLs.

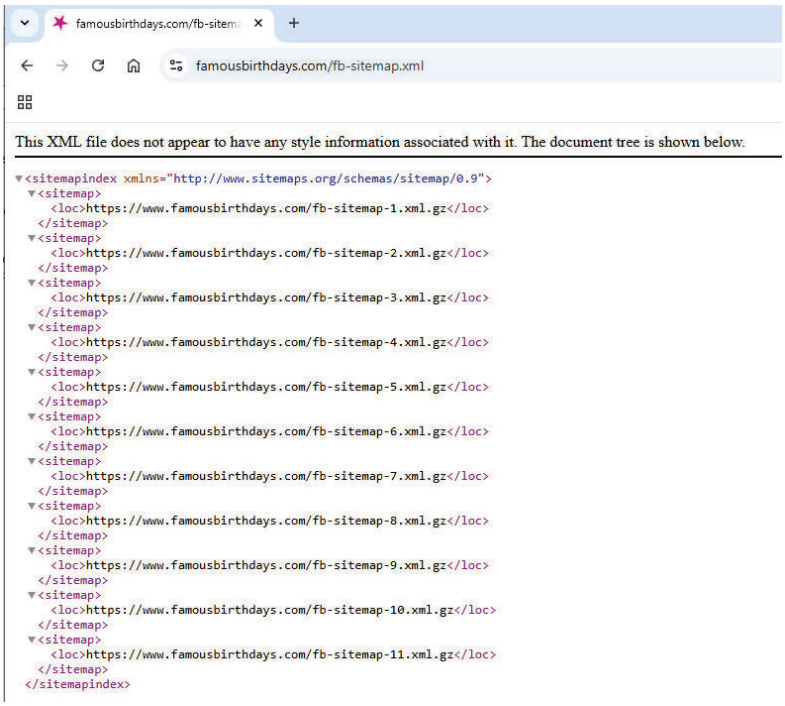
45. Famous Birthdays similarly failed to take any security measures to hide its sitemap for its public website, https://www.famousbirthdays.com/. As such, I also disagree with Famous Birthdays' assertion that "The only way Defendants could have accessed our URL list is by seeking to exploit our sitemap." *See* Ostrowski

Decl., ¶ 33. The URL list can be compiled by any member of the public simply by accessing the HTML that the servers of Famous Birthdays transmit to users as part of their regular operation. Famous Birthdays could restrict access to its URL list by not exposing it to the public but instead maintain the sitemap internally only. However, Famous Birthdays did not restrict access for Passes, or the public for that matter. Any member of the public, even without any access to Famous Birthdays Pro, can access this information by:

i. Navigating to Famous Birthdays robots.txt page, which indicates what data should and should not be indexed by search engines. This page is located at https://www.famousbirthdays.com/robots.txt. A robots.txt file is a text file (or "policy") that website administrators create to instruct search engines on how to interact with their website's pages. It is placed (or published) in the root directory of a website and specifies which parts of the site should or should not be accessed by automated bots. In this context, an indexed page can be found by a search engine based on its content, while a non-indexed page remains "unknown" to the search engine. A robots.txt policy does not express or enforce what pages a user may request, but simply provides guidance to search engines as to what information show and should not be indexed. The last line of the page containing the robots.txt policy says, "Sitemap: https://www.famousbirthdays.com/fb-sitemap.xml". This conveys to any member of the public viewing the robots.txt policy that the server hosts a page that, based on its naming, is the sitemap of Famous Birthdays. Since robots.txt policies are publicly accessible, the Famous Birthdays site map is also publicly visible.



ii. After viewing the robots.txt policy, a user could enter https://www.famousbirthdays.com/fb-sitemap.xml into their web browser would receive the following web page in response:



iii. Entering any of the listed XML URLs in a browser will display the XML document containing a list of URL links.

This information is available to anyone using the internet. Famous Birthdays elected not to place any security measures on members of the public accessing their sitemap. A member of the public accessing the public sitemap absolutely is not "exploit[ing]."

SUMMARY

46. In summary, based on the evidence that I reviewed and that my professional experience, Passes only accessed Famous Birthdays' information that was accessible through the public Famous Birthdays website or through the Famous Birthdays Pro website by using the credentials and/or a token that Famous Birthdays provided to Passes.

47. Further, Famous Birthdays' assertions that Passes "surreptitiously extract[ed] [historical rank graph API call] from the Famous Birthdays source code," or somehow inserted the rank graph API call "amidst Famous Birthdays Pro's source code," are ludicrous, inconsistent with the technical process of making API calls, and entirely unsupported by evidence. Ostrowski Decl., ¶¶ 27, 29.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on November 12, 2024.

DocuSigned by:
/Markus Jakobsson/
CBE08A2A96F04EF...

MARKUS JAKOBSSON